CERIAS Tech Report 2004-44

SCHOOL SAFETY AND THE INTERNET - IS YOUR NETWORK SECURE?

by Dark, M., Iunghuhn M., & Rausch, L.

Center for Education and Research in
Information Assurance and Security,
Purdue University, West Lafayette, IN 47907-2086

School Safety and the Internet - Is Your Network Secure?

Technology is a critical tool in Indiana schools. Schools not only use technology to automate business functions, they are using the tool to process data that drives improvement efforts. The Indiana Department of Education (IDOE) is requiring electronic submission of school and student data, and email has become the communication method of choice. Much of the data that schools collect and use is sensitive. Recently, a California school system was hacked into by a student and grades were changed. Last year, a Russian organized-crime ring used a school network to store stolen credit card numbers. School administrators are becoming concerned about web pages being altered, damaging emails being sent under the school's name, student or staff identity theft, and tampering of confidential records. Sophisticated, but easy to use, hacking tools are readily available on the Internet. Schools are investing scarce resources to build data bases used to drive improvement efforts. Within a few seconds a hacker can destroy hours of work, use a school's network resources to store pornographic pictures, or damage a reputation.

How can schools take preventive measures to ensure this does not happen to them? Last summer, Purdue University's Center for Education and Research in Information Assurance and Security (CERIAS) in partnership with Wabash Valley Educational Service Center decided to investigate the problem by performing "penetration tests" on the networks of five representative school districts in Indiana. Network penetration tests use common vulnerability scanning tools to identify technology system vulnerabilities. In partnership with network security firm, Infotex, permission was obtained from the five districts to perform network penetration tests (i.e., hacked into). A shocking lack of security was found. A testing team was able to hack into all five schools' networks via the Internet. In four of the schools, they accessed payroll and grade information without difficulty, and in three cases they were able to easily obtain a complete list of students and staff. Once inside the internal network, testers were able to circumvent Internet filters using basic tools and techniques well within the grasp of the average middle school student. Perhaps most troubling of all, these attacks and security compromises went undetected because none of the networks contained the necessary staff security tools.

A Holistic Approach

School networking systems have historically been classroom or building systems that were maintained by talented and interested teachers. As the need for more technology increased, the systems grew from building level to district wide systems with full Internet capability. The teachers who once administered the systems have often been replaced by trained network administrators whose responsibilities far exceed those in other industries. Severe time constraints often lead to network security being entrusted to software programs, or obtained as part of a hardware package. Unfortunately, most people still believe this technology is sufficient to address most school security problems. This assumption is false and dangerous; hardware and software alone cannot secure information assets. Just as policy, personnel, and technology are all essential to fulfilling your educational mission, all need to be sufficiently addressed to minimize information security risks (figure 1).

When performing an information security risk assessment, schools should consider a holistic approach (i.e. policy, technology, and personnel). In doing so, they will ensure a process that is consistent and objective while demonstrating the importance of best security practices.

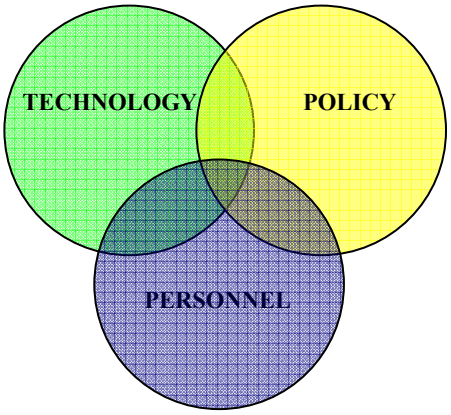

Figure 1: The Holistic Security Approach

The Risk Assessment Process

The principle goal of a school corporation's risk management process is to protect the organization and its ability to perform its mission. A school district's reputation and educational technology assets are also at risk. The risk management process should be completed by a district team that includes staff and students. If your district has never performed a security audit before, then your educational technology system is vulnerable, and now is the time to start the process. An audit should be performed at least once annually and repeated whenever a significant change to the system is made. There are four essential steps (Figure 2) when conducting an information security risk assessment.

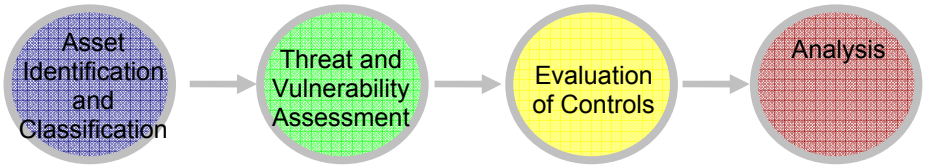

Figure 2: Information Security Risk Assessment Process

Step 1: Identification and Classification. Asset identification and classification is the process of identifying valued assets and categorizing valued possessions of a school into manageable groups. A district could use categories such as hardware and software resources, information resources (grades, health records, attendance records), curriculum resources, and the identity of students, faculty, and staff. By performing asset identification and classification, the information assets that need protection will be clear.

Step 2: Threat and Vulnerability Assessment. Once all assets have been classified, identify the potential threats for each one. Threats are usually classified as natural (storms), human (hackers), or) environmental (power loss). A vulnerability is a weakness that can be accidentally triggered or intentionally exploited. It could be anything from a flaw in the network design to a weakness in the district-wide educational technology policy.

Step 3: Evaluation of Controls. The next step is to preserve the confidentiality, integrity, and availability of your network and data. Controls need to be thought of in terms of whether they prevent, detect, or respond to attacks, and whether they require technical, policy, or personnel oriented counter measures (see Table 1).

Step 4: *Analysis*. The final step is to balance the security needs with the technological needs of the school. The network cannot be so limited by security that it is no longer functional for the students and staff. Network security should be a priority for everyone but not to the point it limits the potential or usefulness of the tool.

Table 1

	Prevention	*Detection*	*Response*
Technology	• Antivirus protection • Access control lists • Firewalls	• Intrusion detection	
Policy	• Acceptable use policies • Systems develop and maintenance policies	• Policies on intrusion response, i.e., roles and responsibilities of your CERT (Computer Emergency Response Team)	• Business Continuity Planning to ensure procedures are in place for bringing the system back online if it is hacked into
Personnel	• Information Security Training		

Summary

Protecting school networks and their data must be a priority for school personnel. Scrutiny of network security practices and policies needs to be a continual process to keep up with the constantly changing network infrastructures and increasingly sophisticated network attacking tools. Students, staff, and administration need to view the implementation of secure network practices and policies as a way to provide a safe and unrestrictive network that allows continual access to necessary resources. A well-conducted information security risk assessment can help accomplish all of these goals.

By
Dr. Melissa Dark Assistant Dean and Associate Professor of Computer Technology Purdue University

Matthew Iunghuhn, Technology Coordinator Wabash Valley Educational Service Center

Dr. Larry Rausch, Executive Director Wabash Valley Educational Service Center